



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/588,049	06/06/2000	MASAKI KYOJIMA	106406	8128
25944	7590	01/06/2005	EXAMINER	
OLIFF & BERRIDGE, PLC P.O. BOX 19928 ALEXANDRIA, VA 22320			LANIER, BENJAMIN E	
			ART UNIT	PAPER NUMBER
			2132	

DATE MAILED: 01/06/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/588,049	Applicant(s) KYOJIMA ET AL.	
	Examiner Benjamin E Lanier	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 07 October 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,3-10 and 12-32 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,3-10 and 12-32 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 06 June 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.
- 13) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.
a) ☐ The translation of the foreign language provisional application has been received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s). _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendment

1. Applicant's amendment filed 07 October 2004 has amended claims 1, 3-5, 8-10, 14, 17, and 19. The amendments to the claims have been fully considered and are entered.

Response to Arguments

2. Applicant's arguments filed 07 October 2004 have been fully considered but they are not persuasive. Applicant's argument that the Boebert reference fails to disclose that the media key/access vector pair is not stored in a memory unit is not persuasive because the storage search logic retrieves the encrypted media key/access vector pair from storage in the personal keying device (Fig. 19 & Col. 16, lines 31-34).

3. Applicant's argument that the Boebert reference does not disclose the enciphered media key/access vector pair is decrypted is not persuasive because Boebert discloses that when retrieved, the encrypted media key/access vector pair is passed to the Key Management Crypto where it is subsequently decrypted by a decryption key generated from the user ID, PIN, and enclave key (Fig. 19 & Col. 16, lines 33-43), of which any or all could represent the second data.

4. In response to applicant's request for an explicit showing of the relationship between the claimed elements of claim 19 and the Boebert reference, the relationships of therefore provided below. The generated data would be the actual media data, and the data generating apparatus would be the media (Fig. 19). The data verifying apparatus would be the crypto media controller (Fig. 19). The reference value memory for holding first data would be the media storage area that stores the media key (Fig. 19). The first data for secondary checking memory unit for holding second data would be area of the personal keying device that stores the access vector (Col. 10,

Art Unit: 2132

lines 36-40 & Col. 15, lines 45-47 & Col. 21, lines 58-63). The decryption key generated from the second data stored in the first data for secondary checking memory unit would be the media key/access vector pair that is ultimately used to decrypt the media data (Col. 16, lines 46-67). The verification unit for checking whether the data decrypted by the decryptor has a prescribed relationship with the first data stored in the reference value memory unit would be the access control logic that uses the access vector to determine whether the user has the appropriate attributes for the desired mode of access (Col. 16, lines 57-61). The data for main checking generation unit for generating third data from the first data sent from the data verifying apparatus would be the storage unit in the personal keying device that stores the media key/access vector that is generated using the media key that comes from the media data (Col. 16, lines 31-34). The second data for secondary checking memory unit for holding fourth data would be the area in personal keying device that stores the user id and/or pin (Col. 10, lines 22-33). The encrypting key generation unit that generates the encrypting key from the fourth data stored in the second data for secondary checking memory unit would be the combined key that is generated from the user id and pin (Col. 10, lines 22-33 & Col. 12, lines 22-24). The encryptor for encrypting the third data generated by the data for main checking generation unit with the encrypting key generated by the encrypting key generation unit would be the media key/access vector that is encrypted with the combined key (Col. 12, lines 22-24).

5. With respect to claim 30, the first device would be the personal keying device which generates the encryption key and encrypts the media key/access vector as disclosed above, and the second device would be the crypto media control that contains the access control logic to validate both the user requesting the data with the media key/access vector pair and the permitted

Art Unit: 2132

access by that user towards the requested data (Col. 16, lines 57-61 & Col. 17, line 60 – Col. 18, line 46).

6. Applicant's argument that the crypto media controller does not decrypt the encrypted media key/access vector pair is not persuasive because Boebert discloses that when retrieved, the encrypted media key/access vector pair is passed to the Key Management Crypto, which is in the crypto media controller (Fig. 19, where it is subsequently decrypted by a decryption key generated from the user ID, PIN, and enclave key (Fig. 19 & Col. 16, lines 33-43).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

8. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

9. Claims 1, 3, 4-10, 12-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boebert, U.S. Patent No. 5,502,766, in view of Deo, U.S. Patent No. 6,496,928. Referring to claims 1, 3, 5, 6, 8, Boebert discloses the claimed limitations. The data for main checking memory unit for holding first data would be the storage unit in the personal keying device that

Art Unit: 2132

stores the media key/access vector that is generated using the media key that comes from the media data (Col. 16, lines 31-34). The data for secondary checking memory unit for holding second data would be the area in personal keying device that stores the user id and/or pin (Col. 10, lines 22-33). The encrypting key generation unit for generating an encrypting key from second data stored in the data for secondary checking memory unit would be would be the combined key that is generated from the user id and pin (Col. 10, lines 22-33 & Col. 12, lines 22-24). The encryptor for encrypting the first data stored in the data for main checking memory unit with the encrypting key generated by the encrypting key generation unit would be the media key/access vector that is encrypted with the combined key (Col. 12, lines 22-24). The data that includes at least one of the result of encrypting by the encryptor and the second data stored in the data for secondary checking memory unit is generated would be the generation of the media key/access vector pair that is encrypted. Boebert does not disclose that the stored keys can be used to generate new keys. Deo discloses the use of old keys that are hashed with other data (data for secondary checking memory unit) to generate new encryption keys (Col. 24, lines 32-54), which meets the limitation of the encryption key generation unit also uses the previous key stored in the previous key memory unit in generating the encrypting key. Deo discloses that the encryption keys are generated using a Message Authentication Code (Col. 24, lines 32-54). Message Authentication Codes are one-way hash functions. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the old keys of Boebert to generate new keys in the manner of Deo in order to increase the difficulty of the key becoming compromised as disclosed in Deo (Col. 24, lines 57-68).

Art Unit: 2132

10. Referring to claim 9, the generated encrypting key from the first data using a one-way function would be combined key that is generated from the user id and pin (Col. 10, lines 22-33 & Col. 12, lines 22-24). The encrypted second data stored in a memory unit with the encrypting key, the second data capable of being checked whether it includes a prescribed characteristic would be the media key/access vector that is encrypted with the combined key (Col. 12, lines 22-24) and the access vector includes access rights for the user (Col. 16, lines 56-61). The data that includes at least one of the result of encrypting by the encryptor and the second data stored in the data for secondary checking memory unit is generated would be the generation of the media key/access vector pair that is encrypted. Boebert does not disclose that the stored keys can be used to generate new keys. Deo discloses the use of old keys that are hashed with other data (data for secondary checking memory unit) to generate new encryption keys (Col. 24, lines 32-54), which meets the limitation of the encryption key generation unit also uses the previous key stored in the previous key memory unit in generating the encrypting key. Deo discloses that the encryption keys are generated using a Message Authentication Code (Col. 24, lines 32-54). Message Authentication Codes are one-way hash functions. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the old keys of Boebert to generate new keys in the manner of Deo in order to increase the difficulty of the key becoming compromised as disclosed in Deo (Col. 24, lines 57-68).

11. Referring to claims 10, 12, 14, 15, 17, The data for main checking memory unit for holding first data would be the storage unit in the personal keying device that stores the media key/access vector that is generated using the media key that comes from the media data (Col. 16, lines 31-34). The data for secondary checking memory unit for holding second data would be the

Art Unit: 2132

area in personal keying device that stores the user id and/or pin (Col. 10, lines 22-33). The decrypting key generation unit comprising a one-way function for generating a decryption key from the second data stored in the data for secondary checking memory unit would be the combined key that is generated from the user id, pin, and enclave key (Col. 16, lines 39-41). The decryptor for decrypting the first data stored in the data for main checking memory unit with the decrypting key generated by the decrypting key generation unit would be decryption of the encrypted media key/access vector pair by the combined key (Col. 16, lines 40-43). The check unit for the checking whether the data decrypted by the decryptor has a prescribed characteristic would be the access control logic that uses the access vector to determine whether the user has the appropriate attributes for the desired mode of access (Col. 16, lines 57-61). Boebert does not disclose that the stored keys can be used to generate new keys. Deo discloses the use of old keys that are hashed with other data (data for secondary checking memory unit) to generate new encryption keys (Col. 24, lines 32-54), which meets the limitation of the encryption key generation unit also uses the previous key stored in the previous key memory unit in generating the encrypting key. Deo discloses that the encryption keys are generated using a Message Authentication Code (Col. 24, lines 32-54). Message Authentication Codes are one-way hash functions. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the old keys of Boebert to generate new keys in the manner of Deo in order to increase the difficulty of the key becoming compromised as disclosed in Deo (Col. 24, lines 57-68).

12. Referring to claim 18, the generated decryption key from first data using a one-way function would be the combined key that is generated from the user id, pin, and enclave key

Art Unit: 2132

(Col. 16, lines 39-41). The decrypted second data with the decrypting key would be decryption of the encrypted media key/access vector pair by the combined key (Col. 16, lines 40-43). The checking whether a result of decrypting includes a prescribed characteristic would be the access control logic that uses the access vector to determine whether the user has the appropriate attributes for the desired mode of access (Col. 16, lines 57-61). Boebert does not disclose that the stored keys can be used to generate new keys. Deo discloses the use of old keys that are hashed with other data (data for secondary checking memory unit) to generate new encryption keys (Col. 24, lines 32-54), which meets the limitation of the encryption key generation unit also uses the previous key stored in the previous key memory unit in generating the encrypting key. Deo discloses that the encryption keys are generated using a Message Authentication Code (Col. 24, lines 32-54). Message Authentication Codes are one-way hash functions. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the old keys of Boebert to generate new keys in the manner of Deo in order to increase the difficulty of the key becoming compromised as disclosed in Deo (Col. 24, lines 57-68).

13. Referring to claims 19, 20, 23-27, 29, the generated data would be the actual media data, and the data generating apparatus would be the media (Fig. 19). The data verifying apparatus would be the crypto media controller (Fig. 19). The reference value memory for holding first data would be the media storage area that stores the media key (Fig. 19). The first data for secondary checking memory unit for holding second data would be area of the personal keying device that stores the access vector (Col. 10, lines 36-40 & Col. 15, lines 45-47 & Col. 21, lines 58-63). The decryption key generated from the second data stored in the first data for secondary checking memory unit would be the media key/access vector pair that is ultimately used to

Art Unit: 2132

decrypt the media data (Col. 16, lines 46-67). The verification unit for checking whether the data decrypted by the decryptor has a prescribed relationship with the first data stored in the reference value memory unit would be the access control logic that uses the access vector to determine whether the user has the appropriate attributes for the desired mode of access (Col. 16, lines 57-61). The data for main checking generation unit for generating third data from the first data sent from the data verifying apparatus would be the storage unit in the personal keying device that stores the media key/access vector that is generated using the media key that comes from the media data (Col. 16, lines 31-34). The second data for secondary checking memory unit for holding fourth data would be the area in personal keying device that stores the user id and/or pin (Col. 10, lines 22-33). The encrypting key generation unit that generates the encrypting key from the fourth data stored in the second data for secondary checking memory unit would be the combined key that is generated from the user id and pin (Col. 10, lines 22-33 & Col. 12, lines 22-24). The encryptor for encrypting the third data generated by the data for main checking generation unit with the encrypting key generated by the encrypting key generation unit would be the media key/access vector that is encrypted with the combined key (Col. 12, lines 22-24). Boebert does not disclose that the stored keys can be used to generate new keys. Deo discloses the use of old keys that are hashed with other data (data for secondary checking memory unit) to generate new encryption keys (Col. 24, lines 32-54), which meets the limitation of the encryption key generation unit also uses the previous key stored in the previous key memory unit in generating the encrypting key. Deo discloses that the encryption keys are generated using a Message Authentication Code (Col. 24, lines 32-54). Message Authentication Codes are one-way hash functions. It would have been obvious to one of ordinary skill in the art at the time the

Art Unit: 2132

invention was made to use the old keys of Boebert to generate new keys in the manner of Deo in order to increase the difficulty of the key becoming compromised as disclosed in Deo (Col. 24, lines 57-68).

14. Referring to claim 22, the commitment random number memory unit for holding a random number would be the authentication token storage unit of the personal keying device (Col. 21, lines 50-52 & 63-67) that holds random number sequences (Col. 26, lines 44-47). The commitment generation unit for generating a commitment from the random number stored in the commitment random number memory unit would simply be the personal keying device which generates authentication tokens from the random number sequences stored in the authentication token storage (Col. 26, lines 44-47). The commitment memory unit for storing the commitment sent from the data generating apparatus could be either the authentication token storage unit of the personal keying device (Col. 21, lines 50-52 & 63-67) or the memory of the authentication token generator (Col. 27, lines 20-24). The data generating apparatus sending the commitment generated by the commitment generation unit to the data verifying apparatus before receiving the first data from the data verifying apparatus would be the authentication protocol for the personal keying device (Col. 27, line 39 – Col. 28, line 32). The data for main checking generation unit, also uses a random number stored in the commitment random number memory unit for generating the third data to be verified and the data verifying apparatus, when its check unit performs checking, also uses the commitment stored in the commitment memory unit is detailed in the authentication protocol for the personal keying device (Col. 27, line 39- Col. 28, line 32).

Referring to claim 4, 13, 21, Boebert discloses that digital signatures can be used in the data enclave system (Col. 23, lines 50-53).

Referring to claims 7, 16, 28, Boebert discloses using symmetric encryption (Col. 9, lines 22 – Col. 10, line 10).

15. Referring to claims 30-32, the first device would be the personal keying device which generates the encryption key and encrypts the media key/access vector as disclosed above, and the second device would be the crypto media control that contains the access control logic to validate both the user requesting the data with the media key/access vector pair and the permitted access by that user towards the requested data (Col. 16, lines 57-61 & Col. 17, line 60 – Col. 18, line 46). Boebert does not disclose using one-way functions. Deo discloses that the encryption keys are generated using a Message Authentication Code (Col. 24, lines 32-54). Message Authentication Codes are one-way hash functions. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the message authentication codes of Deo in the cryptographic methods of Boebert in order to make the system more difficult for an attacker to decipher as taught in Deo (Col. 24, lines 61-65).

Conclusion

16. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E Lanier whose telephone number is 571-272-3805. The examiner can normally be reached on M-Th 7:30am-5:00pm, F 7:30am-4pm.

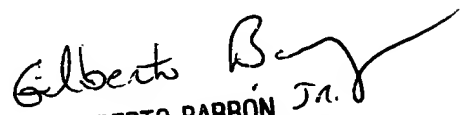
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2132

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Benjamin E. Lanier



GILBERTO BARRÓN JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100